



Prudential Standard CPS 234

Information Security

Objectives and key requirements of this Prudential Standard

This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability that is commensurate with information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity, or availability of information assets, including information assets managed by related parties or third parties.

The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.

The key requirements of this Prudential Standard are that an APRA-regulated entity must:

- clearly define the information-security related roles and responsibilities of the Board, and of senior management, governing bodies and individuals;
- maintain information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- notify APRA of material information security incidents.

Authority

1. This Prudential Standard is made under:
 - (a) section 11AF of the *Banking Act 1959* (Banking Act);
 - (b) section 32 of the *Insurance Act 1973* (Insurance Act);
 - (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act);
 - (d) section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act); and
 - (e) section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

Application

2. This Prudential Standard applies to all ‘APRA-regulated entities’ defined as:
 - (a) **authorised deposit-taking institutions (ADIs)**, including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);
 - (b) **general insurers**, including **Category C insurers**, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and **parent entities of Level 2 insurance groups**;
 - (c) **life companies** including **friendly societies** and **eligible foreign life insurance companies** (EFLICs), and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);
 - (d) **private health insurers** registered under the PHIPS Act; and
 - (e) RSE licensees under the SIS Act in respect of their business operations.¹
3. APRA-regulated entities must comply with this Prudential Standard in its entirety, unless otherwise expressly indicated. The obligations imposed by this Prudential Standard on, or in relation to, a foreign ADI, a Category C insurer or an EFLIC apply only in relation to the Australian branch operations of that entity.
4. Where an APRA-regulated entity is the ‘Head of a group’,² it must comply with a requirement of this Prudential Standard:
 - (a) in its capacity as an APRA-regulated entity;

¹ For the purposes of this Prudential Standard, an ‘RSE licensee’s business operations’ includes all activities as an RSE licensee (including the activities of each RSE of which it is the licensee), and all other activities of the RSE licensee to the extent that they are relevant to, or may impact on, its activities as an RSE licensee.

² Where a Level 2 group operates within a Level 3 group, a requirement expressed as applying to a Head of a group is to be read as applying to the Level 3 Head.

- (b) by ensuring that the requirement is applied appropriately throughout the group, including in relation to entities that are not APRA-regulated; and
 - (c) on a group basis.
5. In applying the requirements of this Prudential Standard on a group basis, references in paragraphs 3, 12 to 36, to an ‘APRA-regulated entity’ should be read as ‘Head of a group’ and references to ‘entity’ should be read as ‘group’.
6. This Prudential Standard commences on 1 July 2019.

Interpretations

7. Terms that are defined in *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001), *Prudential Standard LPS 001 Definitions*, *Prudential Standard HPS 001 Definitions* or *Prudential Standard 3PS 001 Definitions* appear in bold the first time they are used in this Prudential Standard.
8. In this Prudential Standard, unless the contrary intention appears, a reference to an Act, Regulation or Prudential Standard is a reference to the Act, Regulation or Prudential Standard as in force from time to time.
9. Where this Prudential Standard provides for APRA to exercise a power or discretion, this power or discretion is to be exercised in writing.
10. For the purposes of this Prudential Standard:
- ‘group’ means a Level 2 group or a **Level 3 group**, as relevant;
 - ‘Head of a group’ means a Level 2 Head or **Level 3 Head**, as relevant;
 - ‘Level 2 group’ means the entities that comprise:
 - (a) **Level 2** as defined in APS 001; or
 - (b) a Level 2 insurance group as defined in GPS 001;
 - ‘Level 2 Head’ means:
 - (a) where an ADI that is a member of a Level 2 group is not a subsidiary of an authorised banking NOHC or another ADI, that ADI;
 - (b) where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or
 - (c) the parent entity of a Level 2 insurance group as defined in GPS 001.

Definitions

11. The following definitions are used in this Prudential Standard:

- (a) **information asset** means information and information technology, including software, hardware and data (both soft and hard copy);
- (b) **information security** means the preservation of an information asset's:
 - (i) confidentiality, referring to restricting access to that which has been authorised;
 - (ii) integrity, referring to the characteristic of completeness, accuracy and freedom from unauthorised change or usage; and
 - (iii) availability, referring to accessibility and usability when required;
- (c) **information security capability** means the totality of resources, skills and controls which provide the ability and capacity to maintain information security;
- (d) **information security control** means a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;
- (e) **information security incident** means a confirmed or potential compromise of information security;
- (f) **information security policy framework** means the totality of policies, standards, guidelines and procedures pertaining to information security;
- (g) **information security threat** (threat) is a circumstance or event that has the potential to exploit an information security vulnerability;
- (h) **information security vulnerability** (vulnerability) is a weakness in an information asset or information security controls that could be exploited to compromise information security.

Roles and responsibilities

12. The Board of an APRA-regulated entity (the Board) is ultimately responsible for ensuring that the entity maintains the information security of its information assets in a manner which is commensurate with the size and extent of threats to those assets, and which enables the continued sound operation of the entity.³
13. The information security-related roles and responsibilities of the Board, and of senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions, must be clearly defined.⁴

³ A reference to the Board in the case of a foreign ADI, is a reference to the **senior office outside Australia**.

⁴ For the purposes of this Prudential Standard, governing bodies and individuals includes committees, working groups and forums.

Information security capability

14. An APRA-regulated entity must establish an information security capability that meets the requirements of paragraph 12.
15. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.⁵
16. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

Policy framework

17. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.
18. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.⁶

Information asset identification and classification

19. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. Criticality and sensitivity is the degree to which an information security incident affecting that information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

Implementation of controls

20. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:
 - (a) vulnerabilities and threats to the information assets;
 - (b) the criticality and sensitivity of the information assets;
 - (c) the stage at which the information assets are within their life cycle; and

⁵ For the avoidance of doubt, paragraph 15 of this Prudential Standard applies to related parties or third parties not already captured as service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

⁶ For the purpose of paragraph 18 of this Prudential Standard, parties includes governing bodies and individuals with responsibilities referenced in paragraph 13, as well as all other staff, contractors, consultants, related parties, third parties and customers.

- (d) the potential consequences of an information security incident.
21. Where information assets are managed by a related party or third party, an APRA-regulated entity must evaluate the design and operating effectiveness of that party's information security controls.⁷

Incident management

22. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.
23. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).
24. An APRA-regulated entity's information security response plans must include the mechanisms in place for:
- (a) managing all relevant stages of an incident, from detection to post-incident review; and
 - (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.
25. An APRA-regulated entity must annually confirm that its information security response plans are effective.

Testing control effectiveness

26. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:
- (a) the rate at which the vulnerabilities and threats change;
 - (b) the criticality and sensitivity of the information asset;
 - (c) the consequences of an information security incident; and
 - (d) the risks associated with exposure to untrusted environments, where an entity's ability to enforce its information security policy is impeded.
27. Where information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control

⁷ For the avoidance of doubt, paragraph 21 of this Prudential Standard applies to related parties or third parties not already captured as service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

testing, an entity must assess whether that testing is commensurate with paragraph 26 (a)-(d).⁸

28. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner, to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate.
29. Testing must be conducted by appropriately skilled and functionally independent specialists.
30. An APRA-regulated entity must review the sufficiency of the testing program at least annually or on material change to information assets or the business environment.

Internal audit

31. An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).
32. Assurance must be provided by personnel appropriately skilled in providing information security assurance.
33. Where information assets are managed by a related party or third party, internal audit must assess the information security control assurance provided by that party, where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.⁹

APRA Notification

34. An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, after experiencing an information security incident that:
 - (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers; or

⁸ For the avoidance of doubt, paragraph 27 of this Prudential Standard applies to related parties or third parties not already captured as service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

⁹ For the avoidance of doubt, paragraph 33 of this Prudential Standard applies to related parties or third parties not already captured as service providers of outsourced material business activities under *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard SPS 231 Outsourcing*.

- (b) has been notified to other regulators, either in Australia or other jurisdictions.¹⁰
35. An APRA-regulated entity must notify APRA as soon as possible and no later than five business days after identifying a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

Adjustments and exclusions

36. APRA may adjust or exclude any requirement in this Prudential Standard in relation to a particular APRA-regulated entity.¹¹

¹⁰ For the avoidance of doubt, paragraph 34 of this Prudential Standard applies to notifications of information security incidents not already captured as notifications under *Prudential Standard CPS 231 Outsourcing*, *Prudential Standard SPS 231 Outsourcing*, *Prudential Standard CPS 232 Business Continuity Management* or *Prudential Standard SPS 232 Business Continuity Management*. Other regulators include domestic government agencies and international regulators.

¹¹ Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act, subsection 230A(4) of the Life Insurance Act, subsection 92(4) of the PHIPS Act and subsection 34C(5) of the SIS Act.